https://doi.org/10.35147/knpsi.2019.33.2.197

사이버테러 사건 시 디지털 증거 압수·수색에 대한 비교법적 고찰

Comparative Law Study on Confiscation and Search of Digital Evidence as a Countermeasure against Cyber Terrorism

손 창 현*

차 례

● 국문요약 ●

IS의 준동 등 대상을 불문하는 국제적 차원의 테러가 기승을 부리는 가운데 사이버 공간을 대상 그 자체 혹은 수단으로 하여 자행되는 사이버테러 또한 빈발하면서 당해 사이버테러 상황에 보다 효과적이고 긴밀하게 대처하기 위한 다양한 법적·제도적 노력들이 세계 각국들에 의해 시도되고 있다. 이와 관련하여 유효한 디지털 증거를 확보하기 위한 절차의 논의를, 특히 원격 압수·수색 또는 제3자 보관 정보에 대한 압수·수색 방식 등의 현실적 활용이 검토될 필요가 있다. 본고는 2016년 2월 22일 발의되었던 「국가 사이버테러 방지 등에 관한 법률(안)」의 국회통과가 여·야간 첨예한 입장차이로 불발됨에 따라 사이버테러에 적실하게 대응하기 위해 수사 과정에서 현실적으로 활용될 필요가 있는 원격 압수·수색 및 제3자 보관 정보에 대한 압수수색을 「국민보호와 공공안전을 위한 테러방지법」, 이른바 「테러방지법」에 삽입하는 형태로 입법화하는 것이 보다 합리적이라는 전제하에 문제된 압수·수색 방식을 비교법적으로 검토하고자 한다. 이후 이를 대한민국의 특수한 상황 하에서 어떻게 규범의 영역으로 편입시킬 것인지에 대해 살펴본 후 법률 개정에 대한 제언을 하는 형태로 논의를 전개하고자 한다.

* 예비역 공군 헌병대위, 고려대 일반대학원 북한학(통일정책 전공) 박사과정.

◈ 주제어 : 사이버테러, 디지털 증거 원격 압수·수색, 제3자 보관 정보에 대한 압수·수색, 테러방지법, 사이버범죄

Ⅰ. 서론

최근의 테러발생 경향은 종래 물리적 공간에 국한되어 있었던 테러의 양상 또한 보다 네트워크화 되고 다양화된 형태로 전화하고 있다. 결국 전형적 형태의 테러를 상정하여 마련된 기존 테러 방지책만으로는 더 이상 급변하는 테러집단들의 태세전환에 효율적으로 대처할 수 없다는 위기의식이 국제사회를 빠르게 잠식하고 있는 상황 하에 각국은 특히 사이버 공간을 대상 그 자체 혹은 수단으로 자행되고 있는 각종 테러상황에 대응하기 위한 법적·제도적 정비, 기타 노력들을 수행하는 새로운 국면에 돌입하게 되었다.

우리나라 또한 이러한 문제 상황으로부터 자유로울 수 없는 것은 마찬가지여서, 2003년 이른바 1.25 대란이 발발한 이래, 2004년 국가기관 해킹사건, 두 차례에 걸친 북한 발 D-DOS 공격사건 및 그 주체가 북한으로 의심되고 있는 2011년 농협 전산망 해킹사건과 중앙선거관리위원회의 사이버테러사건에 이르기까지 시간이 갈수록 사이버테러 공격이 보다 더 구체화, 현실화되고 있는 실정이다. 문제는 사실 이러한 결과는 대한민국이 처해있는 특수한 안보상황 등을 고려할 때 그 예견이 그리 어렵지 않은 당연한 귀결에 불과하다는 것인데, 그 이유는 첫째, 인터넷 보급률 및 활용도 측면에서 타국과의 그 어떠한 비교도 불허하는 대한민국의 전 국가적 사이버 인프라 구축이야말로 사이버테러를 자행코자 하는 테러집단들에게는 오히려 테러 공간의 확보를 보다

용이하게 한다는 의미에서 일종의 기회라는 것에 있다. 둘째, 긴밀하게 상호 연동되는 전산화 시스템의 경우, 특정 부문에 대한 공격으로 인한 시스템의 마비는 단순히 당해 부문에 한정된 피해를 야기하는데 국한되지 않고 오히려 전 방위적으로, 예측 불가능한 불가역적 대규모 피해를 유발할 수 있다는 것에서 테러집단의 선호를 유인하는 동기로 작동하게 된다는 것이다. 마지막으로 무엇보다 대한민국은 언제든지 최악의 적으로 돌변할 수 있는 잠재적 위험요인인 북한과 지정학적으로 이웃하고 있으며, 따라서 북한에 의한 도발 또는 사전에 예측이 가능한 다양한 방식의 기타 공격에 효과적으로 대비할 수 있는 치밀한 제도적·사회적 방어선 구축이 요구된다.

결국, 복잡다기한 현대 사회에서 테러의 유형이 점차 다양한 형태로 분화되고 있으며, 특히 비용 대비 그 효과가 탁월해 테러집단들에 의해 수용되어 전략적으로 활용될 가능성이 농후한 사이버테러 관련 법안 마련이 시급함에도 불구하고 그 입법화가 불발되었다는 사실은 아쉬움을 남기는 지점이다. 그러므로 본 연구에서는 사이버테러 대응방안으로서의 디지털 증거 원격 압수·수색 및 제3자 보관 정보에 대하여 비교법적으로 고찰하고자 한다.

Ⅱ. 연구 목적 및 진행 방향

사이버테러의 발생 가능성에 주목하고 해당 유형의 테러 대비와 관련하여 종래 진행되어 온 연구들은 크게 두 가지 형태로 준별 가능하다. 우선 사이버테러의 개념을 정의함과 동시에 사이버테러 범죄에 포섭될 수 있는 일련의 행위 유형들에 대한 형법상·특별법상 처벌규정의 분석

에 주력하는 일 형태가 바로 그것이다. 다음으로, 사이버테러에 국한했다기보다는 범죄수사 과정에서 흔히 직면하게 되는 디지털 증거가 종래 증거법을 관통하는 영장주의 기타 법원칙 하에서는 실체적 진실을 발견, 규명하는데 적실하게 사용되고 있지 못함을 지적하고, 이러한 문제점을 해소하기 위한 대안을 구상하는 작업을 수행하는 것이 그 두 번째에 해당한다. 다만 이러한 연구의 경우, 해당 작업이 그 자체로 담보하고 있는 유의미성에도 불구하고 일정한 한계를 노정하고 있음을 부인할 수 없다고 판단된다. 즉 전자의 경우, 테러집단에 의해 자행되는 행위는 비단 테러 그 자체에 한정되는 것이 아니며 최근에는 사이버테러 기타 테러 행위를 보다 용이하게 하는 각종의 보조적 행위, 요컨대 인력채용, 강령의 선전·선동, 자금조달 등이 사이버 공간에서 수월하게 수행되고 있다는 점에서 사이버테러의 개념지형을 더 유연하게 확장할 필요가 있다고 판단된다. 나아가 설령 특정 테러행위가 실체법이 규정하고 있는 범죄 구성요건에 포섭될 수 있다손 치더라도, 유죄의 인정을 가능케 할 수 있는 증거를 수사단계에서 확보할 수 없다면 테러에 대응하는 처벌규정의 확보는 그저 반쪽짜리 대안에 불과하다는 점을 상기할 필요가 있겠다. 다음으로 후자의 경우, 수사단계에서의 디지털 증거의 확보라는, 광범한 주제를 그 대상으로 연구를 진행하다보니 사이버테러와 관련하여 특히 문제되고 있는 구체적 상황에 집중하지 못하고 단순히 원론적인 수준에서 논의가 진행되는 경우가 많았다. 따라서 이러한 점을 종합적으로 고려하여 본고는 다음과 같은 형태로 아래의 논의를 전개해나가기로 한다.

우선, 사이버테러가 사이버 공간에서 자행되는 테러인 만큼 당해 범죄를 특정하고, 유죄를 인정하는데 활용될 수 있는 자료들도 디지털화되어 있을 가능성이 높다는 점을 고려하여, 디지털 증거를 보다 적실하

게 확보하기 위해 각국이 취하고 있는 법적·제도적 입장을 비교법적으로 고찰해보도록 한다.

다음으로, 사이버테러의 경우 디지털화된 정보 그 자체 혹은 당해 정보를 소지하고 있는 주체가 국내에 있느냐, 국외에 있느냐에 따라 그 대응방안을 달리 모색할 수 있는 만큼 양자의 이익 상황이 완전히 동일하지는 않다는 점에 착안하여, 정보 혹은 정보 소지 주체가 국내외의 어디에 속해 있는지 세분화하여 살펴보기로 한다. 이 과정에서 각각의 경우 수사가 종래 어떻게 진행되어 왔는지를 확인하고, 디지털 증거의 효과적 확보를 둘러싼 각국의 정책 상황을 비교법적으로 고찰한 결과를 토대로 유의미한 대안을 모색한 후 제도적으로 제언하고자 한다.

물론 이에 선행하여, 여·야의 정치적 견해가 첨예하게 대립하고 있는 현재와 같은 상황에서는 사이버테러 관련 법안을 독립된 단행법으로 입법화하는 것이 결코 용이하지 않다는 전제 하에, 그렇다면 관련 내용 중 특히 원격 압수·수색 또는 제3자 보관정보에 대한 압수·수색 등 디지털 증거 확보와 결부된 것으로서 그 도입이 시급한 부분을 우선적으로 선별, 기존 「테러방지법」에 삽입하는 형태의 입법화를 모색해보기로 한다.

이러한 작업을 통해 사이버테러의 예방 및 수사에 보다 효과적 대응을 가능케 하는 내용의 정책 제언이 이루어질 수 있을 뿐만 아니라 디지털 증거의 압수·수색과 관련된 다양한 논의들이 현실화될 수 있게 이바지하여 당해 논의들이 장차 입법의 장에 활발하게 호명될 수 있도록 하는데 본고가 기여할 수 있을 것으로 기대된다.

Ⅲ. 현행법의 개정을 통한 입법 방안 모색

1. 현행법이 정하고 있는 개념 정의와 관련된 문제

「사이버테러방지법」안의 경우 테러 방지를 위한 대안 모색의 시급성에는 여·야 공히 동의하고 있으나 동 발의 안 제2조 상 사이버테러의 개념 정의에 대한 입장 차이 및 야당과 시민 연대가 특히 독소조항으로 지목하고 있는 제8조 제2항 상의 '취약점 보고의무' 등에 의한 기본권 침해의 가능성 및 특정 기관에로의 과도한 권한 집중에 대한 우려로 동 발의안과 같거나 유사한 법안이 단행법 차원에서 국회를 통과하는 것은 당분간 매우 요원해 보인다. 그러나 동시에 사이버테러 기타 사이버 공간에서의 관련 범법행위에 대처하여 유효한 디지털 증거를 확보해야할 필요성 또한 갈수록 증대되고 있음은 부인할 수 없는 사실인 바, 단행법 형태로 관련 법안을 정비하는 것보다는 최근 국회를 통과한 「테러방지법」을 개정하여 특정 내용을 삽입하는 것이 보다 효율적이고 현실적인 방안이 될 수 있을 것으로 판단된다.

다만 남과 북이 첨예하게 대치하고 있는 한반도의 특수한 안보 상황하에 사이버테러의 자행 주체가 될 가능성이 높은 북한을 현행 「테러방지법」의 규정상 그 적용 대상에 과연 포함시킬 수 있을 것인지에 관한 정당한 문제제기를 통해 보다 확실한 형태로 북한을 관련 법규 내로 포함시킬 필요가 있다.

2. 사이버테러 관련 현행 「테러방지법」에의 포섭

사이버테러와 관련된 내용을 단행법의 형태로 입법화하기 곤란한 만큼 사이버테러의 예방 및 대처를 위해 필수적인 디지털 증거 확보에 관한 내용을 현행 「테러방지법」 내로 포섭시켜야 한다. 이를 위해 우선 사이버테러에 관한 개념 정의를 동법 제2조 제1호 바목에 신설하여 '테러'개념의 하위개념 형태로 포섭할 필요가 있다. 한편 동법 제9조는 국가정보원장이 출입국, 금융거래 및 통신이용 등 관련 정보와 테러인물에 대한 개인정보 및 위치정보 등을 수집할 수 있다고 명시하고 있는바, 원격 압수·수색 및 제3자 보관정보에 대한 압수·수색 등 해당 내용을 동법 제9조의2로 새로 구성하여 삽입하는 방법이 바람직해 보인다. 관련하여, 우선 사이버테러에 대한 개념 정의에 대해서는 서상기 前 의원이 대표 발의한 「국가 사이버테러 방지 등에 관한 법률(안)」 중 해당하는 부분의 차용을 그 기본으로 하되 본고에서 논의되고 있는 압수·수색 방식을 사이버테러 범죄 전반에 모두 적용하는 것이 입법적으로 부담스러울 수 있다는 점을 고려하여 일정 범죄로 제한할 필요가 있다.[1] 다음으로 디지털 정보의 특성상 기존 압수·수색 방식을 그대로 적용하는 것만으로는 증거로 하기에 부족함이 없을 정도로 유의미한 자료를 압수할 수 없다는 점에서 도입이 요구되는 디지털 증거의 압수·수색에 대해서는 아래 논의를 통해 도출된 결론을 반영하는 형태로 개정을 진

1) 상기 발의 안은 제2조 정의규정에서 사이버테러를 아래와 같이 규정하고 있다.
제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "사이버테러"란 외국이나 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신망을 공격하는 행위를 말한다.

행하여야 할 것이다. 다만 압수·수색의 방법을 온전히 디지털 증거의 속성에만 맞추어 고려하면, 개인의 사생활 등 기본권 및 형사소송법상 절차 즉 영장제시, 참여권 보장 등이 침해될 가능성을 온전히 배제하기 곤란한 측면이 있다. 따라서 적절한 조화가 요청되는 바 사이버테러인 경우와 사이버테러가 아닌 범죄인 경우로 나누어 디지털 증거에 대한 영장 집행방법에 차이를 두면 될 것이다. 또한 동 방식이 야기할지 모를 기본권 등 제한을 최소화하면서 헌법이 기본권 제한을 정당화하는 중요한 가치들 중 하나로 천명하고 있는 국가 안전보장 및 기타 법익을 적실하게 보호할 수 있도록 당해 방식의 적용가능 범죄를 강력한 테러 범죄 등 일정 부분으로 한정하여야 할 것으로 보인다. 또한 일각에서 제기되고 있는 우려를 불식 혹은 최소화시킬 수 있도록 일단의 부수적 조치가 고려, 예비 되어야 한다. 즉 테러단체에 의해 자행될 것으로 예상되는 비위행위는 비단 사이버테러에 해당하는 행위로 국한되는 것이 아니며, 오히려 이러한 테러를 용이하게 하는 다양한 원조행위들이 선행, 혹은 병행될 것으로 봄이 합리적이지만, 그렇다고 영장주의에 위배되는 것으로 평가될 여지가 없지 않은 압수·수색 방식을 테러 관련 비위행위 전체에 전면적으로 적용하려 할 경우 오히려 강력한 반대에 부딪혀 실질적으로 그 도입이 시급한 유형의 범죄 수사에 관해서까지 적용이 배제되는 상황을 초래하는 것은 부조리하다. 따라서 당해 증거확보 방식의 합헌성 및 실효성을 전 범죄에 걸쳐 이익형량하는 경우에 발생할 수 있는 의구심을 적절히 배척하면서 기본권 제한이 용인될 수 있는 일정 범죄유형에 우선 한정하여 동 방식을 규범 영역 안으로 끌어들이는 유연성이 요청된다.

Ⅳ. 비교법적 고찰

1. 필요성

위에서 살펴본 바와 같이 사이버테러는 시간이 지남에 따라 점차 구체화, 현실화되어 실생활에 큰 위협으로 등장하고 있는 반면, 관련 수사를 진행함에 있어서는 난항을 겪을 수밖에 없는 아이러니한 상황에 직면해 있다. 이는 기본적으로 우리나라에서 디지털 증거에 대한 압수·수색이 소극적으로 이루어지고 있기 때문인데, 「형사소송법」은 정보를 명확히 압수·수색의 대상으로 하고 있지 않으며, 판례[2] 역시 저장매체만을 압수·수색의 대상으로 보고 있다. 즉 현행 「형사소송법」은 영장주의 원칙하에 영장에 특정하여 허가받은 유체물에 대해서만 그 압수·수색이 가능한데, 범죄 관련 정보의 소재가 명확하게 특정되어 있지 않은 바에야 컴퓨터용 디스크, USB, 기타 셀 수 없을 정도로 다양한 저장매체를 일일이, 그리고 완전히 특정 하는 것은 사실상 불가능에 가깝다는 것이다. 문제는, 그렇다고 정보 그 자체를 압수·수색의 대상으로 삼는 것 또한 현행 「형사소송법」 규정상 가능한 방식이 아닌 바 저장매체를 온전히 특정하기도, 그렇다고 핵심 관련 정보를 압수·수색의 대상으로 하기도 곤란한 상황에서 수사상 디지털 증거확보를 보다 용이하게 하는 새로운 대안이 등장하지 않는 한, 사이버테러 범죄의 예방 및 대처는 효과적으로 이루어질 수 없다. 결국 이러한 문제의식 하에 디지털 증거 조사와 관련하여 원격 압수·수색과 제3자 보관정보에 대한 압수·수색에

2) 대법원 2015. 7. 16. 2011모1839 전원합의체 결정.

대한 논의가 등장하게 되는 것이다.

따라서 아래에서는 각국이 디지털 정보를 압수·수색의 대상으로 이해하고 있는지를 우선적으로 살펴본 후, 추가적으로 디지털 증거를 어떻게 압수·수색하고 있는지 혹은 그 체계상 제3자 보관정보에 대한 압수·수색을 포함하는 원격 압수·수색에 대해 정책적으로 어떠한 태도를 취하고 있는지 여부를 순차 검토하는 방식으로 비교법적 작업을 수행하고자 한다.

2. 비교법적 분석 1 – 미국의 경우

1) 미국의 디지털 증거 압수·수색 개괄

미국의 디지털 증거를 압수의 대상으로 할 수 있는지에 대한 수정헌법 제4조의 해석과 관련하여 미연방 대법원은 압수·수색의 대상에 전자기록이 포함될 수 있다고 판시하고 있다.[3] 한편, 미 연방 형사소송규칙 제41조는 압수·수색의 대상에 대해 공문, 책, 서류, 다른 만질 수 있는 물건 및 정보를 포함하는 것으로 규정하고 있다.[4] 또한 규칙 41(e)(2)(A)에 의한 영장은 전자적 저장매체의 압수 또는 저장된 정보의 압수 및 복제를 허가할 수 있다고 규정함으로써 저장된 정보의 압수 및 복제가 가능하도록 하고 있다.[5] 나아가 영장에 별도로 기술되지 않는 한 매체

3) United States v. New York Telephone Co. U.S. 159, 169, 98 S.Ct. 364, 54 LEd. 2d376(1997).

4) FRCP 41(a)(2)(A) (A) "Property" includes documents, books, papers, any other tangible objects, and information.

5) FRCP 41(e)(2)(B) A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.

나 정보가 영장의 기재범위와 일치하는지는 사후에 검증할 수 있다. 다만 미국 연방법무부 지침서에 따라 실무적으로는 압수·수색의 방법을 특정하기 위하여 압수·수색의 대상물이 저장매체 그 자체인지, 아니면 저장매체에 저장되어 있는 정보만을 의미하는지를 영장에 특정하여 청구하고 있는 것으로 보인다.

2) 미국의 원격 압수·수색

한편, 미국의 경우 정보에 대한 원격 압수·수색에 관하여 명시적인 규정을 두고 있지는 않다. 다만 미국 연방법무부 지침서에 따르면 네트워크를 수색할 때 압수대상 정보가 여러 관할권으로 분산되어 있는 경우 각 관할권별로 별개의 영장을 받아야 하는 것으로 보인다. 그렇지만 「형사소송규칙」 제41조는 범죄와 관련된 행위가 일어난 지역에 대하여 관할권을 가지는 치안판사 또는 워싱턴D·C에 대한 관할권을 가지는 치안판사는, 해당 주 또는 지역 관할권 외에 소재한 물건에 대하여도 영장을 발부할 수 있다고 규정하고 있어, 각 관할권별로 별개의 영장을 받아야 한다는 규정상의 불편을 해소할 수 있는 길을 열어두고 있다.

3) 미국의 「해외정보감시법」 개괄

특히 미국은 「해외정보감시법(Foreign Intelligence Surveillance Act of 1978, FISA)」을 두어 국가안보와 관련된 디지털 증거 수집이 이 법에 의한 기관에 의해 이루어지도록 규정하고 있으며 외국 세력이나 그 요원들이 나누는 외국기밀정보에 대한 감청 신청이나 통신관련 사실에 대한 제출명령 등은 법원이 아닌 FISA의 지휘 아래 특수절차를 거쳐 이루어지도록 안배하고 있다.

3. 비교법적 분석 2 – 독일의 경우

1) 독일의 디지털 증거 압수·수색 개괄

독일「형사소송법」제94조가 압수·수색의 대상에 대하여 규정하고 있는바 "저장매체 및 그에 저장되어 있는 데이터를 증거의 객체로서 보전 및 압수의 목적물로 하는 것을 허용하고 있으며, 저장매체 및 그에 저장되어 있는 데이터를 수색하고 압수함에 있어서 증명의 의미를 거의 지니지 않는 자료에 대해서는 접근 및 수집을 피해야 하고, 적어도 심각한 고의적 또는 임의의 절차 위반에 의한 압수·수색의 결과로 수집된 저장매체 및 그에 저장된 자료는 증거로서 사용하지 못하게 된다."라고 판시하고 있다. 즉 헌법재판소는 정보인 데이터 증거를 압수의 목적물로 하는 것을 명시적으로 허용하고 있는 것이다. 다만 어디까지나 유관정보만을 그 압수의 대상으로 이해하고 있으며, 설령 예외적인 경우가 있다 하더라도 비례의 원칙 등을 적용하여 기본권 침해를 최소화하는 방향으로 압수할 것을 주문하고 있다. 따라서 비록 독일의「형사소송법」제94조가 '물건'만을 압수의 대상으로 정하였더라도 물건 개념에 데이터 정보까지 포함되는 것으로 해석하여야 할 것이다.

2) 독일의 원격 압수·수색

원격 압수·수색에 관하여「형사소송법」제110조 제3항[6]은 "수색 대

6) StPO §110 (3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein

상자의 전자 저장매체에 대한 검열은 그 검열대상인 데이터가 상실될 우려가 있다면 저장매체로부터 도달될 수 있는 한, 당해 저장매체와 공간적으로 분리되어 있는 저장매체들에까지 확대될 수 있다. 조사에 중요한 의미가 있을 수 있는 데이터는 이를 압수할 수 있다."[7]고 규정하고 있어, 원격 압수·수색에 대한 명문의 근거를 마련하여 두고 있다.

4. 비교법적 분석 3 – 일본의 경우

1) 일본의 디지털 증거 압수·수색 개괄

일본의 경우, 개정을 통해 디지털 증거에 대한 압수·수색 방법 및 기록명령부 압수제도를 도입하였다. 일본「형사소송법」제110조의 2는 전자적 기록 즉 디지털 증거를 담고 있는 기록매체를 압수하는 방법에 대하여 규정하고 있는바 동 규정에 따르면, 압수할 물건이 전자적 기록과 관련된 기록매체인 경우, 압수영장을 집행하는 자는 압수할 기록매체에 기록된 전자적 기록을 다른 기록매체에 복사/인쇄 또는 이전한 후, 당해 다른 기록매체를 압수할 수 있거나 또는 압수를 당하는 자에게 압수할 기록매체에 기록된 전자적 기록을 다른 기록매체에 복사, 인쇄하게 하거나 이전하게 한 후, 당해 다른 기록매체를 압수할 수 있다고 규정하고 있어 미국이나 독일과 같이 정보 그 자체를 압수·수색할 수 있다고 규정하고 있는 것은 아니나, 개정을 통해 특별규정을 두어 전자적 기록에 대해서도 저장매체의 복사본 등을 압수하는 방법으로 해당 정보를 압수할 수 있도록 하였다.

---

können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.

7) 정대용, "수색 대상 컴퓨터를 이용한 원격 압수·수색의 쟁점과 입법론", 법조 65권 3호, 법조협회, 2016, 64쪽.

2) 일본의 원격 압수·수색

일본「형사소송법」제99조 제2항 및 제218조 제2항이 원격 압수·수색과 관련된 내용을 각각 규정하고 있는 바 전자는 "압수할 물건이 전자계산기인 경우, 당해 전자계산기에 전자통신회선으로 접속되어 있는 기록매체로서, 당해 전자계산기에서 작성/수정한 전자적 기록 또는 당해 전자계산기에서 수정/삭제하는 것이 가능한 전자적 기록을 보관하기 위하여 사용되고 있다고 인정하기에 족한 상황에 있는 것으로부터 그 전자적 기록을 당해 전자계산기 또는 다른 기록매체에 복사하여, 당해 전자계산기 또는 당해 다른 기록매체를 압수할 수 있다."고 규정하고 있다. 이는 원거리에 있는 다른 컴퓨터 등에 압수·수색의 대상이 되는 정보가 존재하는 경우, 당해 컴퓨터 등에서 그 다른 컴퓨터 시스템에 접속 가능할 시 압수·수색을 허용하고 있는 것이다. 기록매체로는 당해 전자계산기를 이용하여 작성·수정한 문서 파일을 보관하기 위하여 사용되는 원격 스토리지 서버나 사내 LAN으로 엑세스할 수 있는 파일서버, 당해 전자계산기를 이용하여 전자메일을 보관하기 위하여 사용되고 있는 메일서버 등이 여기에 해당된다.[8)]

5. 소 결

각국이 압수·수색과 관련하여 디지털 증거를 어떻게 이해하고 있는지 비교, 검토하는 작업을 수행하였다. 이러한 과정을 통해 드러난 사실을 요약컨대, 우선 미국은 디지털 증거의 압수·수색 가능성에 대해 법령이

8) 우지이에 히토시, "일본의 전자적 증거 압수에 관한 2011년 개정법 소개", 형사법의 신동향 통권 제49호, 대검찰청, 2015, 422쪽.

명시적으로 규정하고 있는 것은 아니나 판례가 수정헌법 제4조에 대한 해석으로, 전자기록이 압수·수색의 대상이 될 수 있음을 판시함으로써 디지털 증거를 보다 용이하게 확보할 수 있는 길을 열어두고 있는 것으로 보인다. 다음으로 독일의 경우를 보건대, 「형사소송법」이 명시적으로 압수·수색의 대상에 정보를 포섭하고 있지는 않지만 헌법재판소 결정에서, 데이터를 증거객체로서 보전 및 압수의 목적물로 하는 것을 허용하고 있는 등 특이하게도 원격 압수·수색은 독일 「형사소송법」에 그 근거가 마련되어 있다. 마지막으로 일본의 경우에는 「형사소송법」의 개정을 통해 디지털 정보 그 자체는 아니지만 전자적 기록이 담긴 기록매체를 압수·수색할 수 있다고 명시하고 있는 등 원격 압수·수색에 대하여는 일본 개정 「형사소송법」에 그 근거가 있다. 결국 각국은 법률 규정을 통해 정보의 압수·수색 대상성을 인정하고 있는지 여부와 상관없이 디지털 증거확보의 중요성이 빠르게 증대되고 있는 현실과 수사의 실제를 감안하여 수사현실에 부합하는 압수·수색 방식을 모색, 시도하고 있음을 알 수 있다. 이러한 견지 하에 아래에서는 정보 그 자체 혹은 정보의 소지 주체가 국내에 존재하는 경우와 국외에 존재하는 경우로 나누어 각 상황에서 보다 효과적인 디지털 증거확보에 복무할 수 있는 법 제·개정이 가능한지 우선 검토하고, 관련 정책 제언을 하기로 한다.

Ⅴ. 현행 법체계에의 도입 가능성

1. 정보 또는 정보의 소지 주체가 국외에 존재하는 경우

정보 그 자체 혹은 정보의 소지 주체가 국외에 존재하는 경우는 국내에 존재하는 경우와 그 이익상황이 전혀 다르다. 이와 같은 상황은 사

실 범죄가 다양한 국가에 걸쳐 이루어진 경우와 유사하다고 평가할 수 있는데, 세계 각국은 저마다 각자에 맞는 형사절차 및 재판절차를 보유하고 있으므로 주권과 관할권이 주요한 쟁점으로 전면에 등장하게 된다. 기본적으로 국가는 고유의 주권과 사법권으로 자국 내에서 발생한 범죄 혹은 자국민이 행하거나 피해자가 된 범죄를 규율한다. 다만 세계화의 급속한 진행으로 다국적 기업 등 특정 국가에 귀속되지 않는 주체가 등장하기 시작하였고, 정보화의 발달로 클라우드 시스템 등이 구축됨으로써 관련 자료들이 여러 다양한 곳에 산재되어 있는 것이 전혀 어색하지 않은 상황이 되어 버렸다. 이러한 상황 하에서 당해 국가들 간의 긴밀한 공조는 논리필연적인 것으로서, 결과적으로 「국제형사사법공조법」 등이 제정되는 바탕이 되었다.

그리고 그것은 우리나라의 경우도 마찬가지여서, 수사대상에서 벗어나려는 노력의 일환으로 외국에 페이퍼 컴퍼니를 설립하거나 관련 범죄 자료를 해외 서버에 두는 경우가 비일비재해졌으며 중국 등 해외 각지에 거점을 마련하고 국내 국가기관 및 정보기관을 해킹하는 사이버테러 행위가 빈발하여 압수·수색에 어려움을 겪고 있다. 일례로 우리나라는 최근 성인사이트 '소라넷'에 대한 대대적 수사를 진행하면서 네덜란드 암스테르담에 있는 핵심서버를 압수·수색하여 폐쇄하였는데, 이 과정에서 경찰은 수사 초기에는 미국과, 서버가 유럽으로 이전된 이후에는 네덜란드 등과 각 공조하여 수사를 진행하였다. 즉 서버가 해외에 있는 경우에는 단독으로 압수·수색 할 수 없으며, 해당 국가와의 공조수사가 필수적인 것이다. 구체적으로 현행 「국제형사사법 공조법」은 상호주의에 기반하여 제정되었으며, 공조의 개념, 공조의 범위 등에 대해 규정하고 있는바 동법에서 증거 수집, 압수·수색 또는 검증은 공조의 범위에 포함되어 있어, 서버를 비롯해 유관 정보 등이 해외에 존재하는 경

우 이 법에 따라 공조요청을 한 후[9] 압수·수색을 집행하여야 하는 것이고, 이러한 공조 체계를 무시한 채 국내법 수준에서 독단적으로 국외 디지털 자료에 대해 압수·수색 하는 것을 그 내용으로 하는 법을 제정하는 것은 현재로서는 무리한 작업일 것으로 사료된다.

2. 정보 또는 정보의 소지 주체가 국내에 존재하는 경우

1) 원격 및 제3자 보관 정보에 대한 압수·수색의 실제

통상적으로 정보를 압수·수색하는 과정에서는 그것이 원격 압수·수색이 필요한 경우든, 제3자 보관 정보에 대한 압수·수색이 필요한 경우든 관련 상황은 언제든 발생할 수 있으므로 각 압수·수색 방식의 도입 - 만약 실무적으로 양 방식이 이미 활용되고 있다면, 실무적 방식을 뒷받침할 수 있는 법적 근거를 마련한다는 의미에서의 제도적 도입 - 이 필연적으로 요구된다. 주의할 것은 양 방식이 그 자체로 일정한 문제점을 내포하고 있다는 데에 있다. 즉 원격 압수·수색 방식은 최초에 압수·수색 영장을 청구할 당시, 특정하여 기재한 장소와는 전혀 별개의 장소에 있는 대상을 압수한다는 점에서 영장주의 원칙에 위배될 수 있다. 또한 제3자 보관 정보에 대한 압수·수색 방식의 경우에는 정보의 주체와 정보의 소지 주체가 서로 다르기 때문에 당해 정보주체인 피의자의 참여권이 충실히 보장되기 곤란한 측면이 있다. 따라서 아래에서는 해당 방식이 담보하고 있는 문제가 과연 극복 불가능한 성질의 것인지 우선 검토하고, 나아가 현행법상의 개선방향으로서 개정과 관련해 어떠한 제언을 할 수 있는지 검토하기로 한다.

9) 국제형사사법공조법 제29조(검사의 공조요청) 검사는 외국에 수사에 관한 공조요청을 하려면 법무부장관에게 공조요청서를 송부하여야 하고, 사법경찰관은 검사에게 신청하여 법무부장관에게 공조요청서를 송부하여야 한다.

2) 원격 압수·수색 방식 검토

기실 원격 압수·수색의 필요성에 대해서는 학설대립과 무관하게 모든 학자들이 동의하고 있는 바이다. 디지털 정보라는 것이 그 성질상 복사, 삭제, 이동이 용이하고, 인터넷 네트워크를 통해 산재되어 존재하는 것이 가능하며, 나아가 클라우드 서비스를 통해 정보 소지자의 통제 하에 있더라도 그가 직접 점유하지는 않는 상태로 정보가 존재하기도 하는 만큼 종래의 물리적 공간 및 유체물을 특정하여 압수·수색하는 형태의, 기존 영장집행 방식으로는 이와 같은 극적인 변화를 온전히 대응하지 못하기 때문이다. 그럼에도 불구하고 이러한 방식의 압수·수색을 반대하는 견해를 무조건적으로 배척할 수는 없는 것이, 원격 압수·수색에 정확하게 맞아떨어지는 명문 규정이 존재하지 않고, 당해 압수·수색으로 인한 개인의 사생활 침해 등 문제가 야기될 수도 있기 때문이다. 따라서 디지털 증거를 압수·수색할 수 있도록, 특히 원격지에 대한 압수·수색이 가능하도록 법률 개정 혹은 제정 작업이 수행되어야 한다. 결국 ①원격 압수·수색이 기존 영장주의에 포섭될 수 있으며 그러한 점에서 결과적으로 기본권을 침해한다고 보기 어렵다고 이해하는 경우는 물론이거니와 ②해당 방식이 현행 법체계 내에 자연스럽게 포섭될 수 있는 것이 아니기에 후속적으로 기본권 보장 및 영장주의의 실현이라는 당위의 측면과 수사 실제 및 실체 진실 발견이라는 필요의 양 측면을 이익형량하여야 하는 과정이 요구되는 경우에도, 적절한 균형점을 찾아 양 가치를 조화롭게 반영한 규정을 신설하는 것이 법적으로 불가능한 것은 아니라고 판단된다. 즉 법률 개정 작업을 수행하는 와중에도 영장주의라는 헌법적 가치는 훼손되지 않아야 한다는 것인데, 결국 당해 방식으로 취급되는 정보는 기본적으로 범죄의 혐의가 있는 것이어야 하고, 특히 범죄의 혐의 있

는 유관정보에 국한되어야 할 것이다. 이와 같은 점을 고려하여 테러방지법에 새로운 조문을 신설하면 다음과 같을 것이다.

「테러방지법」 제9조의2 제1항 "전자정보의 압수 목적으로 컴퓨터 등 정보처리장치(이하 '컴퓨터 등'이라 한다)를 수색하는 경우 압수할 전자정보가 연동된 다른 컴퓨터 등에 기억되어 있다는 사정 및 명확히 유관정보로 인식될 수 있는 경우에 한하여 다른 컴퓨터 등에 대한 수색을 할 수 있다. 다만, 압수·수색의 목적·대상·기간이 특정되어야 하며, 다른 컴퓨터 등에 대한 수색은 합리적인 범위 내에서 이루어져야 한다.

3) 제3자 보관 정보에 대한 압수·수색 관련 검토

실무적 차원에서 제3자 보관 정보에 대한 압수·수색은 매우 빈번하게 이루어지고 있다. 기본적으로 현행 「형사소송법」 제215조는 사법경찰관의 검사에로의 영장 신청, 검사의 법원에로의 영장 청구를 통해 법원이 발급한 영장에 의해서 압수·수색할 수 있음을 규정하고 있다. 한편 「통신 비밀보호법」 제6조 및 제13조는 필요한 경우 법원의 허가를 받아 범죄수사를 위한 통신제한조치를 할 수 있도록, 혹은 범죄수사를 위한 통신사실 확인자료의 제공을 구할 수 있도록 각 규정하고 있다. 그리고 이러한 규정들은 각자가 그 적용대상으로 삼는 객체를 달리하고 있는바 이메일, 가입자 정보, 금융거래내역, 가상 저장 공간 내 저장된 파일 등은 「형사소송법」상의 압수·수색 영장에 의해서, 반면 로그기록, 통화내역, 기지국 정보 등은 「통신비밀보호법」상 명시하고 있는 법원의 허가서와 통신사실 확인자료 제공요청에 의해 각 압수된다.[10] 문제는

10) 이정희, "제3자 보관 디지털 증거의 압수 관련 문제점 및 개선방안 연구", 박사 학위논문, 고려대학교 일반대학원, 14쪽.

실무적으로 대부분의 수사기관이 위 허가서와 영장을 판사로부터 발부받은 후, 압수할 장소에 방문하여 직접 영장을 제시·집행하지 않고, 정보통신서비스제공자 혹은 금융기관 등 디지털 증거를 저장·보관하고 있는 제3자에게 모사전송(FAX)을 통해 영장을 전송한 후 데이터를 이메일로 회신 받는 방식으로 영장을 집행하고 있다는 것이다.[11] 실제로 이러한 방식으로 이루어진 통신사실 확인자료 제공요청만 해도 2018년 기준 총 68,468건에 달할 정도로 매우 빈번하다.[12]

비교컨대, 원격 압수·수색의 경우에는 애초에 영장에 기재되어 있지 않은 장소에 존재하는 정보에 대한 압수·수색이 이루어진다는 점에서 영장주의의 본질적인 부분과 관련한 논란이 촉발될 여지가 있다. 그러나 제3자 보관 정보에 대한 압수·수색의 경우에는 발부된 영장이 특정하고 있는 바와 같이 그 정보를 보유하고 있는 제3자에 대하여 압수·수색이 집행된다는 점에서 이러한 문제가 발생하지 않는다. 따라서 이러한 측면에 주목한다면 영장을 직접 제시하지 않고 모사전송하거나, 디지털 정보를 출력·복제하지 않고 이메일로 전송받는 등의 소위 엄밀하게 영장주의의 본질적인 부분과 관련되어 있다고 보기에 조금 애매한 구석이 있다. 반면, 동 압수·수색의 집행이 제3자에 대하여, 그리고 그 정보가 저장되어 있는 장소에서 이루어진다는 점에서 피압수자가 이런 사실을 알기 어려우므로 참여권이 침해되는 등의 문제가 발생할 여지가 있다. 관련하여, 현행 「형사소송법」 제106조 제4항이 정보주체에게 압수·수색 사실을 지체 없이 알려야 함을 명시적으로 규정하고 있는 것은 물론, 그 적용 객체가 완전히 동일하지는 않지만 디지털 정보라는 측면에서 그 이익상황이 다소 유사한 「통신 비밀보호법」의 경우에 "검사 또는 사법경찰관이 일정기간 공

11) 이정희, 앞의 보고서, 18쪽.
12) 대법원 홈페이지, 사법통계의 "기타영장".

소를 제기하거나 제기하지 않기로 하는 처분이 있은 후 30일 내에 가입자에 대해서 통지"하도록 하고 있음에도 제3자 보관 정보에 대한 압수·수색이 실무상 진행되는 경우 이러한 통지 기타 참여권이 제대로 보장되지 않아 제3자 아닌 정보주체가 사전 혹은 사후에 이를 인지하기 어려운 상황에 빈번히 처하게 된다는 것은 아쉬운 지점이다.

따라서 제3자 보관 정보에 대한 압수·수색의 경우 정보주체의 참여권을 적실하게 보장한다는 전제 하에, 영장주의의 본질적인 부분을 훼손하고 있는 것은 아닌 실무 관행을 감안하여 새롭게 법을 개정할 필요가 있다. 이때 정보주체에로의 통지와 관련하여, 「형사소송법」 제106조 제4항을 쫓을 것인지, 「통신 비밀보호법」 상 통지를 쫓을 것인지를 검토해야 하는 바, 「테러방지법」 내 사이버테러 행위는 일반 사건에 비해 그 중대성이나 시급성이 월등하고, 만약 지체 없이 압수·수색 사실을 통지할 경우 추가적 증거 확보가 요원할 수 있다는 사정들을 종합적으로 고려할 때 참여권 자체를 포기하지 않으면서도, 동일한 취지에서 규정된 「통신 비밀보호법」상 통지 절차를 따르는 것이 보다 바람직하다고 판단된다. 이러한 사정을 감안하여 다음과 같이 새로운 조항을 제정할 수 있을 것이다.

「테러방지법」 제9조의2 제2항 "테러위험인물에 대한 제3자 보관 정보에 대하여 압수·수색을 집행한 경우에 그 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다."

「테러방지법」 제9조의2 제3항 "제2항의 압수·수색을 집행하는 경우 영장의 직접 제시는 모사전송으로, 정보의 출력 또는 복제는 암호화된 이메일 등 전자기록(이하 '이메일 등'이라 한다)의 형식으로 각각 갈음할 수 있다."

Ⅵ. 결론

본고는 디지털 증거의 적실한 확보를 위해 각국이 마련하고 있는 법적·제도적 장치들에 대해 검토하였다. 이는 현행 테러방지법에 관련 내용을 삽입하는 형태의 개정을 추진하는 것이 보다 합리적이라는 전제하에, 디지털 정보 그 자체 혹은 정보 소지 주체가 국내에 있는지, 국외에 있는지로 각 경우의 수를 나누어 관련 실무를 확인한 후, 특히 전자의 경우 정보에 대한 원격 압수·수색 및 제3자 보관 정보에 대한 압수·수색과 관련하여 현행 법제를 정비할 만한 지점을 확인, 개정을 제언하였다. 영장주의의 몰각 및 국민의 기본권 침해 우려를 불식하면서 실체진실을 발견하고, 국가 안전보장 기타 질서유지라는 또 다른 헌법적 가치 실현을 위해 대한민국 사회가 납득할 수 있는 수준과 정도의 압수·수색 방식을 최종 구상·기획하였다. 테러의 유형이 다양한 형태로 분화발전되고 있으며 수법이 탁월하여 테러집단들에 의해 활용됨을 효율적으로 차단할 수 있는 현실적인 사이버테러 관련 법안 마련이 시급하여 사이버테러 대응방안으로서의 디지털 증거 원격 압수·수색 및 제3자 보관 정보에 대하여 비교법적으로 고찰한 결과로부터 다음과 같은 결론을 얻었다.

1. 사이버테러의 위협은 대한민국의 특수한 안보상황과 맞물려 더욱 확연하게 그 실체를 드러내고 있으며, 따라서 당해 사태에 직면하여 테러 상황을 예비, 대처하기 위한 수사 방식, 그 중에서도 특히 수사의 실제 및 실체적 진실발견을 적실하게 담보하기 위한 원격 압수·수색 기타 제3자 보관정보에 대한 압수·수색 등 보다 유연한 압수·수색 방식의 도입이 강하게 요구된다.

2. 현행 테러방지법에 관련 내용을 삽입하는 형태의 개정을 추진하는 것이 보다 합리적이라는 전제 하에, 디지털 정보 그 자체 혹은 정보 소지 주체가 국내에 있는지, 국외에 있는지로 각 경우의 수를 나누어 관련 실무를 확인한 후, 특히 전자의 경우 정보에 대한 원격 압수·수색 및 제3자 보관 정보에 대한 압수·수색과 관련하여 현행 법제를 정비할 만한 지점을 확인, 개정을 제언하였다.
3. 영장주의의 몰각 및 국민의 기본권 침해 우려를 불식하면서 실체 진실을 발견하고, 국가 안전보장 기타 질서유지라는 또 다른 헌법적 가치 실현을 위해 대한민국 사회가 납득할 수 있는 수준과 정도의 압수·수색 방식을 구상·기획할 필요가 있다.
4. 부디 하단의 <현행법/개정안 대조표> 방식의 개정을 통해 사이버테러를 보다 효과적으로 봉쇄하거나 당해 상황이 야기하는 다양한 위협에 효과적으로 대응할 수 있는 사법적 기반을 공고히 할 수 있을 것으로 기대해본다.

〈현행법/개정안 대조표〉

	현행(現行)	개선안(改善安)
정의 규정	테러방지법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. "테러"란 국가 · 지방자치단체 또는 외국정부(외국 지방자치단체와 조약 또는 그 밖의 국제적인 협약에 따라 설립된 국제기구를 포함한다)의 권한행사를 방해하거나 의무 없는 일을	테러방지법 제2조(정의) 1. "테러"란 국가 · 지방자치단체 또는 외국 정부(외국 지방자치단체와 조약 또는 그 밖의 국제적인 협약에 따라 설립된 국제기구를 포함한다)의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 다음 각 목의 행위를 말한다. 바. "사이버테러"란 외국이나 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단, 해킹 · 범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹 · 컴퓨터 바이러스 · 서비

	현행(現行)	개선안(改善安)
	하게 할 목적 또는 공중을 협박할 목적으로 하는 다음 각 목의 행위를 말한다. 가.-바. (바목 신설)	스방해 · 전자기파 등 전자적 수단에 의하여 정보통신망을 공격하는 행위를 말한다. 단, 형법 제2편중 제1장 내란의 죄, 제2장 외환의 죄중 제92조 내지 제101조의 죄 및 국가보안법에 규정된 범죄에 한정한다.
	테러방지법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 2. "테러단체"란 국제연합(UN)이 지정한 테러단체를 말한다. 가. (신설) 나. (신설)	테러방지법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 2. "테러단체"란 다음의 단체를 말한다. 가. 국제연합(UN)이 언급한 결의안에 포함된 테러단체 나. 대남 적화통일을 목적으로 활동하는 반국가단체
압수 · 수색 방식	테러방지법 제9조의2(원격 압수 · 수색) ①-③ 신설	테러방지법 제9조의2(원격 압수 · 수색) ① 전자정보의 압수 목적으로 컴퓨터 등 정보처리장치(이하 '컴퓨터 등'이라 한다)를 수색하는 경우 압수할 전자정보가 연동된 다른 컴퓨터 등에 기억되어 있다는 사정 및 명확히 유관정보로 인식될 수 있는 경우에 한하여 다른 컴퓨터 등에 대한 수색을 할 수 있다. 다만, 압수 · 수색의 목적 · 대상 · 기간이 특정되어야 하며, 다른 컴퓨터 등에 대한 수색은 합리적인 범위 내에서 이루어져야 한다. ② 테러위험인물에 대한 제3자 보관 정보에 대하여 압수 · 수색을 집행한 경우에 그 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 자에게 압수 · 수색 · 검증을 집행한 사실을 서면으로 통지하여야 한다. ③ 제2항의 압수 · 수색을 집행하는 경우 영장의 직접 제시는 모사전송으로, 정보의 출력 또는 복제는 암호화된 이메일 등 전자기록(이하 '이메일 등'이라 한다)의 형식으로 각각 갈음할 수 있다.

〈논문접수 : 2019. 8. 2, 심사개시 : 2019. 8. 6, 게재확정 : 2019. 9. 9.〉

참 고 문 헌

Ⅰ. 국내 문헌

1. 단행본

곽병선 외, 사이버 수사 및 디지털 증거수집 실태조사, 국가인권위원회 용역과제, 2012.

대검찰청, 압수·수색 관련 판례의 태도 및 외국 증거법제 도입가능성 연구, 2014.

2. 논문

박민우, “디지털 증거 압수수색에서의 적법절차”, 박사 학위논문, 고려대학교 일반대학원, 2016.

우지이에 히토시, “일본의 전자적 증거 압수에 관한 2011년 개정법 소개”, 형사법의 신동향 통권 제49호, 대검찰청, 2015.

윤지영, “미국 수사기관의 온라인 감시에 대한 비판적 연구”, 형사법의 신동향 통권 제39호, 대검찰청, 2013.

윤해성, “사이버테러의 동향과 대응방안에 관한 연구”, 연구총서 12-B-03, 한국형사정책연구원, 2012.

이관희, “디지털정보 취급에 관한 형사절차 개선방안”, 석사학위논문, 고려대학교 정보보호대학원, 2012.

이숙연, “형사소송에서의 디지털증거의 취급과 증거능력”, 박사학위논문, 고려대학교 일반대학원, 2010.

Ⅱ. 외국 문헌

Jansen, W., Grance T., “NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing”, NIST(November, 2013).

Joel Samaha, “Criminal Procedure(9thed.)”, Wadsworth, Vol. 79, No. 3(September, 2015).

< ABSTRACT >

Comparative Law Study on Confiscation and Search of Digital Evidence as a Countermeasure against Cyber Terrorism

Son, Chang-Hyeon

IS cyber terrorism, which is carried out by itself or as a means of cyber space, is also frequent in the face of international terrorism, regardless of whether it is a target of cyber terrorism, institutional efforts are being sought by countries around the world. In this regard, it is necessary to examine the practical use of the discussion of procedures for securing effective digital evidence, for example, confiscation and search methods for remote seizure or search or third party archiving information. This paper compares on the premise that it would be more rational to legislate in the form of inserting the remote seizure, search and seizure search of third-party information into the "Terrorism Prevention Act for National Protection and Public Safety" to respond to cyber terrorism faithfully. I would like to review it legally. After this, we will examine how to incorporate this into the area of norm under the special circumstances of the Republic of Korea, and then propose a revision of the law.

◈ Key words : Cyber terrorism, Cyber Crime, The National Anti-Terrorism Act, A legislative Bill on National Anti-Terrorism Act, Digital Evidence